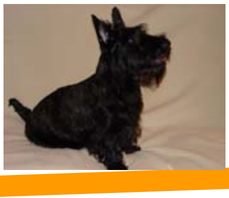


IDACS Quarterly Newsletter

Volume 1, Issue 3

3rd Quarter 2004

INSIDE THIS ISSUE:

Hits –to –Wants

System users are reminded that when possible the FBI number should be included in a wanted person entry. When the NCIC wanted person file entry contains the FBI number, the same wanted information is posted on the subject's FBI Interstate Identification Index (III) criminal history record. If the FBI receives subsequent arrest fingerprints that are identified with the criminal history record, the NCIC system sends an automatic notification message to the agency that entered the warrant.

This message is referred to as a hits-to-wants message and informs them the wanted person has been arrested.

Users must ensure that proper follow-up is conducted when an agency receives one of the hits-to-wants messages, as they can provide valuable leads in the apprehension of a wanted subject. The wanting agency should contact the arresting agency to determine if the subject is still in custody. If the subject has been released from custody, it is possible the arresting agency has knowledge of the subject's whereabouts and apprehension on the warrant may still be possible. If the physical location of the subject is no longer known, the hits-to-wants notification message may provide valuable information, such as additional alias names the subject may be using.

```
*****REFERENCE ARREST IN ANYTOWN, IN (ORI/IN0000000)*****

TO:  SHERIFF'S OFFICE
        ANYTOWN, IN
NCIC CONTROL TERMINAL OFFICER - FOR INFORMATION

ON 2004/06/02, ARREST FINGERPRINT CARD FOR DOE,JOHN J.
WITH DOB OF 19580715, DATE OF ARREST 2004/05/23 AND LOCAL IDENTIFICATION
NUMBER 123456 WAS IDENTIFIED WITH FBI/12123P2.  SUBJECT ARRESTED
BY SHERIFF'S OFFICE  (ORI/IN0000000), OURTOWN.   OUR
RECORDS INDICATE YOUR AGENCY HAS AN ACTIVE WANT FOR THIS INDIVIDUAL
AS DOE, JOHN JOSEPH, CASE NUMBER 98765, ENTERED
IN NCIC (NIC/W123456789).  SUBJECT'S IDENTIFICATION RECORD,
INCLUDING CURRENT ARREST INFORMATION, IS AVAILABLE VIA THE
INTERSTATE IDENTIFICATION INDEX.  FOLLOW-UP ACTION BY YOU WITH
THE ARRESTING AGENCY MAY BE APPROPRIATE.

CLEAR OR CANCEL YOUR NCIC RECORD WHEN SUBJECT NO LONGER WANTED.

FBI CJIS DIVISION
CLARKSBURG, WV
```

Indiana Missing Children's Clearing House

The Indiana General Assembly established the Indiana Missing Children Clearinghouse (IMCC) in 1985. The Clearinghouse is intended to serve as the State Central Repository for all information on missing children from Indiana or believed to be in Indiana. The IMCC is located within the Indiana State Police Headquarters.

Federal and state law forbids the establishment of a waiting period for reporting a missing child.

Indiana Code 10-13-5-4 defines the criteria for designating a missing child as:

1. Under the age of 18 years old.
2. Believed to be a temporary or permanent resident of Indiana.
3. At a location that cannot be determined by the person's parent or legal custodian.
4. Reported missing to a law enforcement agency.

Or a temporary or permanent resident of Indiana; and a victim of the offense of criminal confinement or interference with custody. **Federal and state law forbids the establishment of a waiting period for reporting a missing child.**

Indiana Code 31-36-1-1 thru 31-36-1-4 – defines law enforcement's responsibilities as:

1. Prepare a report on the missing child that includes information that the law enforcement agency determines is relevant that is obtained in the course of the notification about the missing child, including physical description, date and place of birth, name and address of the last school attended by the child, if any.
2. Maintain information or evidence gathered by a preliminary investigation, if one was made.
3. **Include a statement by the law enforcement officer in charge setting forth that officer's assessment of the case based upon the evidence and information received.**
4. **Not later than fifteen (15) days after completion of the report, the law enforcement agency shall forward the contents** of this report to the last:

(1) child care center or child care home in which the child was enrolled; or
(2) school the child attended in Indiana; if any:
if the child is less than thirteen years of age.

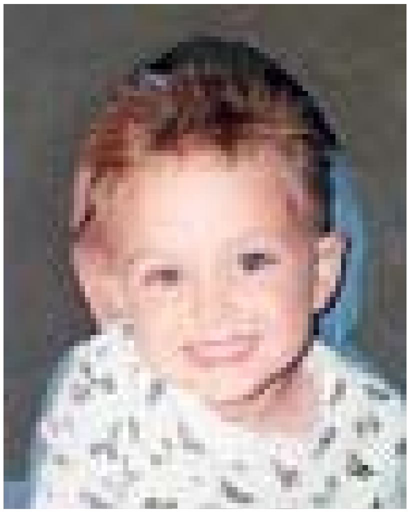
Along with sending the IMCC a case report as mandated by IC 31-36-1-3, the Clearinghouse should also be provided a photo of the missing child. The photo, the child's name, and the agency handling the case, will be published on the state's website **(www.state.in.us/isp)** and in the state's quarterly Missing Children Bulletin. Additional information may be obtained by calling the MCCH at 1-800-831-8593.

NAME : NOAH LEE SPENCER TURNER
ALIAS:
DATE MISSING: 07/09/03
LOCATION LAST SEEN: 1887 N CR50 E, Logansport, IN
DESCRIPTION: Noah is a white male (date of birth 07/15/99). At the time of his disappearance, he was 3'4" tall and weighed 33 lbs. He has blonde hair and blue eyes.

IDENTIFYING INFORMATION: Has lazy eye when tired. He should be wearing glasses.
CLASSIFICATION: MISSING PERSON - ENDANGERED Taken by the mother

CONTACT:

Trooper J.R. Carmin
State Police Redkey Post
R.R. 1, Redkey, IN 47373
(765) 369-2561
case # 25-14396



Validation Codes

A problem that has been occurring with the Omnixx system is the settings for each device. It is imperative that the Validation Code, Agency , and Omnixx Path is made available at each workstation in your agency to insure that the device will function properly. The correct information must be affixed to each device in a prominent location.

To obtain this information for each device, go to the Omnixx Log-In screen. On the Log-In screen, next to the USERNAME and Password is a link marked "click here for more details". That link will drop down the Agency, Validation Code, and Omnixx Path information. The Agency will always be IN, the Validation Code will be different for each device, and the Omnixx Path will always be C:/.

On more than one occasion operators have put their agency's initials in the place of IN in the Agency Field and their ORI as the Validation Code. If the Omnixx path is changed from C:/ to something else, the message log and search capabilities will become inoperable.

To avoid any of these problems affix the proper settings on or near each device so all operators will have access if needed. This should also help eliminate any problems or help avoid unnecessary calls to Coordinators, IDACS and Data Operations.

"I can't get my screens to open, help!"

U.S. Department of State Bulletin Diplomatic Plates in the U.S.

Due to the large number of unaccounted for Department of State (Diplomatic) license plates in the "KV" series, the State Department has required the owners of vehicles bearing plates in this series to exchange their current plates for plates bearing a different two-letter code.
The vehicle owners were given 60 days to comply with this requirement. They were also warned that at the end of the 60-day period, any plates that have not been exchanged will be deregistered and the plate numbers will be entered in NCIC as stolen (Federal) property.
The 60-day period expired March 26, 2004. Any vehicle bearing diplomatic plates in the "KV" series should be considered an unregistered vehicle" being operated in violation of current U.S. laws.

Officer are requested to confiscate these plates and to arrange their return to the Department of State. The point of contact is: Clay Hays 202-895-3544 (daytime) or 202-647-7277 (after hours).

Using the NOA Field

The NOA Field, also known as Notify Originating Agency of all Hits, is sometimes used by agencies in order to track a subject even though the subject may have been stopped outside of the assigned pickup area indicated on the warrant.

The NOA Field will automatically default to "N" for "NO". If an agency chooses to use the NOA Field, then "Y" for Yes must be used. If "Y" is used then the agency that entered the subject will receive notification each time another agency inquiries on the entered subject. The NOA replaces NOAH that was used in the MIS Field.

Driver's License Search and Photo Request

A screen is now available to obtain a driver's license search. This screen replaces the previous (AM) message procedure that was used to obtain driver's license information when a DOB, SOC or any other numerical data was not known.

If a name has been obtained on an individual and other identifiers are needed, a search can now be requested by a DNQ request. Indicate the two letter state code that the search is to be processed through followed by the NAM (name) of the individual (Last name, First, Middle Initial). If an age, sex, the city or county is known, enter that data into the appropriate fields. Once the information is transmitted, a manual check will be preformed and the response will be sent back to the requesting agency. An automatic response will not be received right away.

An IMQ (Image Request) is available on driver's license screens. A state has to be participating in order for an image to be returned. If an image is requested place "Y" in the IMQ field. Automated Images are not available on Indiana Driver's Licenses at this time, however, if a photo is needed requests can be sent to ISP Operations.

Requests for an Indiana BMV digital picture and/or signature can be submitted to the Indiana State Police, GHQ, Operations Section. The requests may be submitted via (AM) message (INISP0005), in person, fax (317-232-0652) or by e-mail opedl@isp.state.in.us, Requests submitted need the following information:

1. Subject's name and date of birth (exactly as it appears on the driver's license).

2. Subject's driver's license number.

3. Indiana BMV Transaction Number.

4. The Transaction Date

5. Requesting officer's last name and identification number.

6. Reason for request (example: case number, incident number, or UTT number)

7. A call back number, for any questions, concerning the request.

For quickest response it is recommended that your request be sent via e-mail. Questions can be directed to the Operations Section at 317-232-8250.

For more information consult the NLETS Manual, Chapter 8. The NLETS Manual is available under Help on the toolbar of the Omnixx Force Program.

Accessing the IDACS Newsletter

The IDACS Newsletter is now available on the Omnixx System. Adobe 5.0 or a higher version can be use to obtain the newsletter. It can be obtained when signed onto Force and is listed under Help on the menu bar. The drop down menu is listed as IDACS News. The newsletter is also available at www.in.gov/isp/idacs. The newsletter will no longer be mailed due to the availability on line. It will be the responsibility of the coordinator of each agency to disseminate the contents of the newsletter to all authorized personnel as well as the non-terminal agencies your agency services that may not have access to the internet. The retention period for the newsletter is three (3) years.

Validation and purges

Policy

The policy for validation has not changed see (240 IAC 5-2-7 Validation of records).

Procedure

The procedure for providing the records for validation in IDACS/ NCIC has changed.

On or about the 20th of the current month IDACS will send a message, over the system, advising the number and type of record(s) to be validated for the following month. This will include the non-terminal agencies that the terminal agency provides service to, if any.

The agency can retrieve the records to be validated by going to FORMS, then to IDACS, then to VALIDATIONS, and Request Validation Record Data (QVAD) form.

All records must be validated by midnight of the last day of the month the record is due to be validated.

Have you ever wondered, " Have I validated all of my records?" Validated records are removed from the validation list. GREAT NEWS, you can use QVAL (summary of records to be validated) form to check if there are any records left to validate. It is recommended that a QVL be ran on or about the 25th of the month, only those records that have not been validated will be on this report. To retrieve the record use the VAD Form.

<u>Purges</u>

1. Annual:
   This purge is for records that reach their retention period and occurs in January. Guns, Unidentified, Missing and Wanted Person remain in file until the entering agency removes the record.
2. Monthly Validation:
   Records not validated.
3. Located Records:
   Purged when the retention period for the record that is located is reached.
4. Expired Protective Orders:
   Protective Order purged on the expiration date, unless the expiration date is changed.
5. Missing Person:
   Purged when a single Locate is placed on the record.

It is the responsibility of the terminal agency coordinator to see that the non-terminal agency receives a copy of those records to be validated.

<u>Non-terminal Agency Validations</u>

It is the responsibility of the terminal agency coordinator to see that the non-terminal agency receives a copy of those records to be validated.

Records still to be Validated

It is recommended that a QVL (summary of records to be validated) be ran on or about the 25th of the month. To make sure that all of the records for the current month are validated, cleared, or canceled. This will let you know if there are records still to be validated.

IDACS Salutes Clay Carter

In life, we all meet people that have an immediate impact on our lives or jobs. Some bloom into lifelong friendships and working relationships that move mountains. The IDACS community has been blessed with many such individuals, who have refused to sit on the sidelines and instead, rolled up their sleeves, shared their knowledge and experience, and was part of the moving the state's communication and data system into the 21st century. Clay Carter is one of those unsung heroes, and today it is truly a privilege to honor him with "this song".

Clay was hired on the Huntington County Sheriff's Department on December 4, 1984 as a dispatcher. Through his tenure in law enforcement, he has made several achievements. He was a member of the Disaster Action Team for the Huntington Red Cross, the civil defense and member of APCO as well as President during 2000-2001. He also served on the IDACS Committee from May 16, 1991 to approximately June 10, 1997. Through his six years on the committee he served as liaison between the agencies in Area II and IDACS. His dedication and knowledge to serve the IDACS community was extremely useful.

Clayton Carter

Clay currently resides in Huntington County with his wife Hazel of 37 years. They have 5 children, 7 grand children and one great grand child. He is a member of the First Christian Church in Andrews and was a past member and president of the Andrews Town Board.

His hobbies include camping, working on his home computer and developing his own family pictures on the computer. For the past twelve years, Clay has held the position of head of the Communications Section for Huntington County Sheriff and holds the rank of Captain.

The past and present efforts and dedication from individuals like Clay Carter have helped in the IDACS System as well as the IDACS Community. His help has been greatly appreciated over the years and the IDACS Community applauds him.

Encryption, Authentication, and Access Control - Digesting the Alphabet Soup of Network Security

In any discussion of Network Security, one is likely to hear a myriad of terms floating about; some unfamiliar and some familiar, but used in unfamiliar ways. Nonetheless, network security really boils down to three primary concepts: encryption, authentication, and access control. This article will try to help you understand what each of these concepts mean in the context of network security.

Encryption

The most discussed concept in regards to CJIS network security is ***encryption***. While authentication and access control have been requirements for CJIS for quite some time, the requirement that data be *encrypted* is relatively new to the CJIS framework. As mentioned in the last newsletter, the latest version of the CJIS Security Policy states, All FBI CJIS Division's information passing through a public network segment must be protected with encryption, while in that segment …"

CJIS Security Policy, Version 3.2, August 2003, p. 13

So what is encryption? Encryption is a method of protecting the *content* of a message so that it cannot be understood if intercepted improperly. Similar to the "coded messages" used in World War II, encryption replaces the characters we see on the screen with other computer codes by following a pattern of replacement called an *algorithm*. A simple algorithm for illustration purposes might be:

"Replace every character in an even-numbered position with the character five positions later in the alphabet, and replace every character in an odd-numbered position with the character five positions earlier in the alphabet. Replace numbers using the same pattern."

Encryption, Authentication, and Access Control - Digesting the Alphabet Soup of Network Security (Continued)

Using this algorithm, the phrase "Hello World 123" becomes "Cjgqj Rtmqy, 678." Quite unintelligible, is it not? However, if you know the algorithm, it is fairly easy to translate this back into the original phrase. Of course, industry standard encryption algorithms like the Defense Encryption Standard (DES-3, where the "3" simply means it is applied three times over itself), and the newer Advanced Encryption Standard (AES, also known as "Rijndael", pronounced like "rain doll") use much more complex rules for encryption, but this example should give you a good idea of what happens.

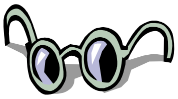
Authentication

While encryption protects the data from being understood if it is intercepted "in the open," ***authentication*** and its related concept ***identification*** protect systems by limiting who can use the systems and in what ways they may use its functions. You encounter identification and authentication every time you use your ATM card at a bank machine. At a bank machine, you insert your card into the machine to tell the bank whose account to access. But then, you also enter a *personal identification number* or PIN to verify that you are the person using the card is the actual owner of the account. Suppose someone steals your purse or wallet with your ATM card? Without your PIN, which you should always keep secret, your card will not work at a bank machine, will it? The thief may have your *identification*, but without the matching *authentication*, your money is kept safe.

In the CJIS network, identification is handled by your *user ID*, while your *password* serves to authenticate you as the true owner of that particular user ID. Just as with your bank card, these pieces of information must be carefully guarded and not shared with others. In the same way a thief can impersonate you and drain your bank account if he has your card and PIN, sharing your user ID and password makes it possible for someone else to impersonate you as they access the system, possibly running transactions that could later place you in serious, even criminal liability for what was done under your identification and authentication.

Access Control

As the third leg of the stool of network security, ***access control*** protects the machines within which systems like Omnixx operate. Access control is typically established through the use of a ***firewall***. A firewall functions like the walls of a fortress with a drawbridge at a guarded gate providing the only way for traffic from outside the fortress to get within its walls. Your agency's network, including your workstation, is the town that the fortress protects. The firewall administrator functions as the gatekeeper, who knows in advance what traffic is safe to allow inside the walls; all other traffic is kept out until it can prove itself trustworthy and safe.



Firewalls operate from lists of rules that specify what messages are deemed safe to allow in, based upon what machine the message comes from and where it was sent to and even what program it is meant for on that machine. A firewall can be a program running on your machine, but most often a firewall is a dedicated machine in the path of the network traffic, through which all traffic must pass to continue on. With a firewall, attempts to access weakness in your machines programs from outside hackers can be prevented by blocking the routes those attacks typically take. No business network attached to **the Internet** should be without a firewall to protect it. In fact, CJIS Security Policy makes it a requirement that: "Networks in which some terminals, or access devices have CJIS access and/or Internet access (e.g., peer-to-peer relationships, large mainframes and servers that house websites) ***must be protected by firewall type devices*** that implement a minimum firewall profile, to provide a point of defense and a controlled and audited access to servers, both from inside and outside the CJIS networks."

CJIS Security Policy, Version 3.2, August 2003, p. 18 *(emphasis added)*

Putting It All Together

Working together, ***encryption, identification/authentication,*** and ***access control*** *can* protect your data, systems and machines from unauthorized access, use and infiltration. But they only *will* work if **you** do your part. If you are a terminal Agency Coordinator or a network administrator, ensure that proper levels of encryption are in place if your network is shared with other non-law enforcement entities (see "Mixed Company – Is Your Network Public?", IDACS News Quarterly, Volume 2004, Issue 1); enforce policies against user ID and password sharing; and implement and monitor a strong firewall to prevent unauthorized access to your network and its machines. And if you are a CJIS user, make sure that ***no one has access to your user ID or password!*** Together, we can all keep CJIS system integrity and security at its highest!

Indiana State Police
IDACS Section
IGCN- 100 N. Senate Ave.
Indianapolis, IN 46204 -2259

Phone: 317-232-8292
Fax: 317-233-3057
Email: idacs@isp.state.in.us

WWW.IN.GOV/ISP/IDACS

Everything Happens For The Good

There was once a King who had a wise advisor. The advisor followed the King everywhere, and his favorite advice was, “Everything happens for the good”. One day the King went hunting and had a little accident. He shot an arrow at his own foot and was injured. He asked the advisor what he thought about the accident, to which the advisor replied, “Everything happens for the good”. This time the King was really upset and ordered for his advisor to be put in prison. The King asked his advisor, “Now, what do you think?” The advisor again replied, “Everything happens for the good”. So the advisor remained in prison. The King later went on a hunting trip, this time without the advisor. The King was then captured by some cannibals. He was taken to the cannibals' camp where he was to be the evening meal for the cannibals. Before putting him into the cooking pot he was thoroughly inspected. The cannibals saw the wound on the King’s foot and decided to throw him back into the jungle. According to the cannibals' tradition, they would not eat anything that was imperfect. As a result the King was spared. The King suddenly realized what his advisor said was true. The advisor also escaped death because had he not been in prison, he would have followed the King on the hunting trip, and would have ended up in the cooking pot.

Success Principles

It is true that everything in life happens for a purpose, and always for our own good. If you think about it, all our past experiences actually happened to bring us to where we are today, and it is always for the good. All the past experiences makes us a better person. So, whatever challenges that we may face today, consider it happening to bring us to the next level.

IDACS Staff

IDACS System Coordinator
Michael Dearinger

Program Director
Andre’ Clark

Administration
Holly White (Working Leader)
Sara Bloemker

IDACS Training
Kelly Dignin
Vivian Nowaczewski
Troy Scott

IDACS Security
Sgt. John Clawson
Sgt. John Richards

Data Operations Center Staff

Supervisor
Carrie Hampton

Day Shift (0700-1500)
Eric R. Macy (Working Leader)
Ala Munn
Lajuan Harris

Evening Shift (1500-2300)
Patsity Epps (acting Working Leader)
Sherif (Leldo Ba) Lee

Night Shift (2300-0700)
Brian Thayer (Working Leader)
Wayne Swift
Fred M. Kline